JOURNAL OF ALGEBRA 19, 51–79 (1971)

Modular Representations of Classical Lie Algebras and Semisimple Groups

J. E. HUMPHREYS*

Courant Institute of Mathematical Sciences, New York University, New York 10012

Communicated by N. Jacobson

Received April 30, 1970

INTRODUCTION

Let K be an algebraically closed field of prime characteristic p. By a *classical Lie algebra* over K we shall here understand a Lie algebra $\mathfrak{g}$ obtained from a complex *simple* Lie algebra $\mathfrak{g}_{\mathbf{C}}$ by the well-known procedure of Chevalley (see Refs. [1] and [15]). In this paper, we discuss some aspects of the representation theory of $\mathfrak{g}$ over K, announced earlier in Ref. [8], and then apply these results to the study of indecomposable modules for semisimple algebraic groups. All modules considered will be finite dimensional, unless otherwise indicated.

Our main technical device is the systematic use of certain p^m-dimensional cyclic $\mathfrak{g}$ modules, denoted Z_λ (m = number of positive roots). After some preliminary results in Sections 0–2, the exposition continues in two essentially independent directions, culminating in, respectively, Theorems 3.1, 4.1, 5.1, and Theorem 4.4. The former theorems explore the relationship (which we call "linkage") between highest weights of composition factors in an indecomposable module, while the latter theorem relates the modules Z_λ to the principal indecomposable modules of the restricted universal enveloping algebra of $\mathfrak{g}$. Finally, Theorem 4.5 brings these two chains of reasoning together. Some complements are provided in Sections 6 and 7.

The assumption that the root system is *irreducible* avoids a few technical complications, but is not really essential. The transition to the general case is almost immediate: The Lie algebra attached by Chevalley's process to a semisimple complex Lie algebra is actually a *direct sum* of algebras of the

* Visiting Member, Courant Institute of Mathematical Sciences, during 1969–1970, with support of Sloan Foundation. Part of this research was done during a stay at the Institute for Advanced Study, and at Queen Mary College (London).

type we consider, being the Lie algebra of a direct product of simply connected Chevalley groups of simple type [15, Section 5].

0. Preliminaries

Let Σ be the (irreducible) root system of $\mathfrak{g}_{\mathbf{C}}$ relative to a Cartan subalgebra $\mathfrak{h}_{\mathbf{C}}$, and let $\Pi = \{\alpha_1, \ldots, \alpha_l\}$ be a simple system. Fix a Chevalley basis $\{X_\alpha, \alpha \in \Sigma; H_i, 1 \leqslant i \leqslant l\}$ of $\mathfrak{g}_{\mathbf{C}}$; if $\mathfrak{g}_{\mathbf{Z}}$ is the $\mathbf{Z}$ span of this basis, then by definition $\mathfrak{g} = \mathfrak{g}_{\mathbf{Z}} \otimes K$. For convenience, we also denote by X_α and H_i the corresponding basis elements of $\mathfrak{g}$. Write $\mathfrak{h} = \mathfrak{h}_{\mathbf{Z}} \otimes K$ (= span of the H_i in $\mathfrak{g}$). Using Kostant's theorem [1, Theorem 1.4; 15, Section 2], which describes a $\mathbf{Z}$ basis of the $\mathbf{Z}$ form $\mathscr{U}_{\mathbf{Z}}$ of the universal enveloping algebra $\mathscr{U}_{\mathbf{C}}$ of $\mathfrak{g}_{\mathbf{C}}$ generated by all $X_\alpha^m/m!$ ($\alpha \in \Sigma$, $m \geqslant 0$), one is able to construct an *admissible lattice* (lattice stable under $\mathscr{U}_{\mathbf{Z}}$) in an arbitrary $\mathfrak{g}_{\mathbf{C}}$ module. In particular, let V_λ be an irreducible $\mathfrak{g}_{\mathbf{C}}$ module of highest weight λ, and let $v_0 \in V_\lambda$ be a *maximal vector* (a nonzero weight vector annihilated by all X_α, $\alpha \in \Pi$); then $\mathscr{U}_{\mathbf{Z}} v_0$ is an admissible lattice, the unique smallest $\mathbf{Z}$ form of V_λ, which includes v_0 and is stable under $\mathscr{U}_{\mathbf{Z}}$. Tensoring with K yields a restricted $\mathfrak{g}$ module $\overline{V}_\lambda$, which is simultaneously a module for the simply connected Chevalley group G constructed from $\mathfrak{g}_{\mathbf{C}}$ over K. If v_0 again denotes the maximal vector $v_0 \otimes 1$ in $\overline{V}_\lambda$, then v_0 has weight λ, where "weight" refers either to a linear function on $\mathfrak{h}$ or to a rational character on the corresponding maximal torus T of G (the former being the differential of the latter); it is convenient to allow λ to mean either of these notions, depending on context.

It is easy to see that the G module $\overline{V}_\lambda$ is cyclic, generated by v_0 [15, p. 212, exercise (c)]. This would not necessarily be the case if we chose a different admissible lattice (cf., [15, p. 212]); nevertheless, the composition factors of the resulting G module (multiplicities counted) always coincide with those of $\overline{V}_\lambda$. This is analogous to a theorem of Brauer–Nesbitt [7, 82.1] for modular group representations obtained by reduction mod p. The proof is not difficult: The sum of weights (with multiplicities) occurring in V_λ is an element of the weight lattice attached to $\mathfrak{h}_{\mathbf{C}}$ invariant under the Weyl group W of $\mathfrak{g}_{\mathbf{C}}$; this lattice identifies canonically with the character group $X(T)$ of T, on which the Weyl group of G (which is again W) acts accordingly; but W-invariant elements of $X(T)$ are expressible *uniquely* as integral combinations of the weight sums associated with the irreducible modules for G.[1] In what follows, we shall be concerned only with $\overline{V}_\lambda$ (and with this only at a couple of points).

Let Λ denote the collection of p^l *restricted* weights λ characterized by the

[1] See, for example, J. P. Serre, "Groupes de Grothendieck des schémas en groupes réductifs déployés," Sect. 3.6, Publ. Math. I.H.E.S. no. 34, 1968.

conditions $0 \leqslant \lambda(H_i) < p$, $1 \leqslant i \leqslant l$. For each $\lambda \in \Lambda$ let M_λ be a (restricted) irreducible $\mathfrak{g}$ module of highest weight λ; it is known that M_λ is a homomorphic, but not always isomorphic, image of $\bar{V}_\lambda$. The collection $\mathscr{M} = \{M_\lambda \mid \lambda \in \Lambda\}$ exhausts the (isomorphism classes of) restricted irreducible $\mathfrak{g}$ modules; each M_λ is also an irreducible G module, and in fact all irreducible G modules are obtainable by Steinberg's method as "twisted" tensor products of these [1, Theorem 7.5; 14, Section 5; 15, Section 12].

Let $\hat{\mathscr{U}}$ and $\hat{\mathscr{H}}$ be the respective universal enveloping algebras of $\mathfrak{g}$ and $\mathfrak{h}$ over K, and let $\mathscr{U}$ and $\mathscr{H}$ be the restricted universal enveloping algebras (u algebras), of respective dimensions $p^{\dim \mathfrak{g}}$ and p^l. (Left) $\mathscr{U}$ modules correspond precisely to restricted (left) $\mathfrak{g}$ modules. We remark that *any u-algebra is Frobenius*, a fact which will enable us to use some standard information about multiplicities in Section 4; see Ref. [11] for reference to this theorem of A. Berkson.

Finally, we record here some elementary observations about the structure of a finite-dimensional commutative, associative algebra A over K, which are very special cases of theorems in Ref. [7]. The radical of A is just the collection of nilpotents in A, and the semisimple algebra $\bar{A} = A/\operatorname{rad} A$ is uniquely expressible as a direct sum of ideals $\bar{A}\bar{e}_i$ (each isomorphic to K), where the $\bar{e}_i$ are uniquely determined primitive idempotents. Lifting, we get A expressed as the direct sum of indecomposable ideals Ae_i, where it is easily seen that the idempotents e_i are uniquely determined. Therefore, there is a unique semisimple subalgebra of A complementary to $\operatorname{rad} A$ (a "Wedderburn factor"), viz., $Ke_1 + \cdots + Ke_t$ ($t = \dim \bar{A}$). A has exactly t maximal ideals, each the kernel of an irreducible representation of A (under which the appropriate e_i is sent to 1), and the intersection of these ideals is $\operatorname{rad} A$.

1. Standard Cyclic Modules and Characters

Definition. A cyclic G module, or $\mathfrak{g}$ module, generated by a maximal vector (of weight λ) will be called *standard cyclic* (of weight λ).

We noted above that for any weight λ, $\bar{V}_\lambda$ is a standard cyclic G module. Using a technique borrowed from lectures of A. Borel [1, proof of Theorem 6.4], we can deduce from this the following fact.

Proposition 1.1. *If $\lambda \in \Lambda$, the $\mathfrak{g}$ module $\bar{V}_\lambda$ (constructed from the admissible lattice $\mathscr{U}_{\mathbf{Z}} v_0$) is standard cyclic of weight λ, generated by v_0.*

Proof. The operator $X_\alpha^i/i!$ on V_λ preserves the lattice, hence, defines an operator $X_{\alpha,i}$ on $\bar{V}_\lambda$ (which is simply $X_\alpha^i/i!$ if $i < p$, but which cannot be so represented if $i \geqslant p$). Then the operation of the unipotent element $x_\alpha(t)$ of G

on $\bar{V}_\lambda$ is given by $\sum_{i\geqslant 0} t^i X_{\lambda,i}$. We shall need the following commutation rules, to be read off first in $\mathscr{U}_{\mathbf{Z}}$ [1, (1.4), (5.14)]:

$$X_{\alpha,i}X_\beta = X_\beta X_{\alpha,i} + \sum_{j>0} c_j X_{j\alpha+\beta} X_{\alpha,i-j}, \qquad \alpha \neq \pm\beta,$$

$$X_{\lambda,i}X_{-\alpha} - X_{-\alpha}X_{\lambda,i} \in \mathscr{A}X_{\alpha,i-1},$$

$$X_{\lambda,i}\mathscr{A} = \mathscr{A}X_{\lambda,i}.$$

Here $\mathscr{A} = \mathscr{A}_{\mathbf{Z}} \otimes 1$, $\mathscr{A}_{\mathbf{Z}}$ the subring of $\mathscr{U}_{\mathbf{Z}}$ with 1 generated by all $\binom{H_i}{n_i}$ as in Ref. [15, Section 2].

Now let V be the $\mathfrak{g}$ submodule of $\bar{V}_\lambda$ generated by v_0. Since v_0 generates $\bar{V}_\lambda$ as G module, it will suffice to show that V is stable under the action of G. For this it suffices in turn to show that $x_\lambda(t)$ stabilizes V for all $\pm\alpha \in \Pi$, $t \in K$. Now the assumption that $\lambda \in \Lambda$ is equivalent to the statement that for α *simple*, the weight string λ, $\lambda - \alpha$, $\lambda - 2\alpha$,... terminates before we reach $\lambda - p\alpha$. In particular, $x_{-\alpha}(t)v_0 \in V$, i.e., $X_{-\alpha,i}v_0 \in V$ for all $i \geqslant 0$. Since $X_\alpha v_0 = 0$, it is equally true that $X_{\alpha,i}v_0 \in V$ for all $i \geqslant 0$. Proceed now step-by-step, with fixed $\alpha \in \Pi$: Let $w \in V$ be such that $X_{\pm\alpha,i}w \in V$ for $i \geqslant 0$. If $\beta \in \Sigma^+$ our commutation formulas (and induction on i) show that $X_{\pm\alpha,i}X_{-\beta}w \in V$ for $i \geqslant 0$. Now V is spanned by the vectors

$$X_{-\beta_1}^{i_1} \cdots X_{-\beta_m}^{i_m} v_0, \qquad 0 \leqslant i_j < p,$$

for an arbitrary ordering of the m positive roots $\beta_1, \ldots, \beta_m$, because the u algebra $\mathscr{U}$ has a Poincare–Birkhoff–Witt (PBW) basis. Our argument, therefore, shows that all $X_{\pm\alpha,i}$ ($\alpha \in \Pi$, $i \geqslant 0$) stabilize V, so G does. Q.E.D.

It is obvious that a standard cyclic G module V of weight λ is indecomposable, since the weight space for λ is one dimensional; this also forces V to have a unique maximal submodule viz. the sum of all proper submodules (= sum of all proper standard cyclic submodules). But some collapsing of weights may occur when we take differentials, so that λ may occur with greater multiplicity than one. In spite of this, Braden is able to prove the following [4]:

PROPOSITION 1.2. *A standard cyclic* $\mathfrak{g}$ *module* V (*restricted or not*) *is indecomposable and possesses a unique maximal submodule.*

Proof. Let v_0 be a maximal vector of V. The Poincaré–Birkhoff–Witt theorem implies that V is spanned by vector monomials (*) $X_{-\gamma_1} \cdots X_{-\gamma_t} v_0$, where $\gamma_1, \ldots, \gamma_t$ is any string of positive roots (repetitions allowed.) To this vector in V, we may assign a "level" $\sum_i$ level (γ_i), where the level of a positive root is the sum of coefficients in its expression as a linear combination of

simple roots. Different ways of writing (*) may lead to different levels (e.g., when (*) is zero), but the levels assigned to *nonzero* vector monomials in V are *bounded*, since the subalgebra $\mathfrak{n}'$ of $\mathfrak{g}$ spanned by negative root vectors is nilpotent. Now choose a basis B for V consisting of v_0 together with other vector monomials. Suppose V is decomposable: $V = V_1 \oplus V_2$, and write $v_0 = v_1 + v_2$ ($v_i \in V_i$). At least one of the v_i must have nonzero v_0 component cv_0 (relative to the basis B), say v_1. Then we claim that $V_1 = V$. Otherwise, at least one nonzero vector monomial (*) lies outside V_1, and we choose it to have highest possible level (among all possible ways of expressing all possible vector monomials outside V_1). Then $X_{-\gamma_1} \cdots X_{-\gamma_t} v_1 \in V_1$, and this vector is the sum of $cX_{-\gamma_1} \cdots X_{-\gamma_t} v_0$ (which is nonzero and outside V_1) along with various vector monomials of strictly higher level (which lie in V_1 by choice of (*)), whence a contradiction. Our argument proves not only that V is indecomposable, but also that every proper submodule of V lies in the subspace spanned by $B - \{v_0\}$. Therefore, the sum of all proper submodules of V is distinct from V, hence is the unique maximal submodule of V. Q.E.D.

Remarks. (1) It seems to be an open question whether the unique maximal submodule of V in Proposition 1.2 must be generated by maximal vectors, but examples computed by N. Burgoyne suggest a negative answer.[2]

(2) The $\mathfrak{g}$ module $\overline{V}_\lambda$ in Proposition 1.1 is restricted, since the corresponding linear Lie algebra in $\mathrm{End}(\overline{V}_\lambda)$ is precisely the Lie algebra of the linear group representing G on $\overline{V}_\lambda$. Since we are ultimately interested in the modular representations of G, *we assume henceforth that all representations of* $\mathfrak{g}$ *under consideration are restricted*; so the notions of $\mathfrak{g}$ module and $\mathscr{U}$ module will be equivalent.

(3) In his thesis (see [3]) and in more recent unpublished work [4], Braden has discussed for types A_2 and B_2 the composition factors of the $\mathfrak{g}$ modules $\overline{V}_\lambda$. The results, while they confirm a general principle to be formulated below (see Theorem 4.1), are rather complicated, and the direct methods used to obtain them appear to be very difficult to extend to higher ranks (or even to G_2). N. Burgoyne has recently developed an efficient method for computing composition factors in individual modules; his examples in ranks 2, 3, 4 become rather more complicated than Braden's.

In characteristic 0 the "most general" standard cyclic module for $\mathfrak{g}_\mathbf{C}$ is always infinite-dimensional; the structure of such modules is studied in detail by Verma in his thesis [16, 17]. Here we shall consider the analog for $\mathfrak{g}$, borrowing some notions from Verma, Cartier, and Harish-Chandra *et al.*

[2] Cf., the analogous Theorem 1 of Ref. [17]; however, Braden observes that the proof given in [16] is incomplete. *Added in proof*: A counterexample has recently been found by I. I. Bernstein, I. M. Gel'fand, and S. I. Gel'fand.

If $\{\beta_1, \ldots, \beta_m\}$ is the set of positive roots, let $X_1, \ldots, X_m$ and $Y_1, \ldots, Y_m$ be the corresponding X_{β_i} and $X_{-\beta_i}$, respectively. As standard PBW basis for $\mathscr{U}$, take the monomials

$$Y_1^{i_1} \cdots Y_m^{i_m} H_1^{j_1} \cdots H_l^{j_l} X_1^{k_1} \cdots X_m^{k_m}, \qquad 0 \leqslant i_s, j_s, k_s < p.$$

Let $\mathfrak{n}$ and $\mathfrak{n}'$ be the subalgebras of $\mathfrak{g}$ spanned by the X_i and Y_i, respectively, and let $\mathscr{N}$ and $\mathscr{N}'$ be their u algebras.

If $\lambda \in A$, denote by I_λ the left ideal in $\mathscr{U}$ generated by all X_i, $1 \leqslant i \leqslant m$, and all $H_i - \lambda(H_i) \cdot 1$, $1 \leqslant i \leqslant l$. Set $Z_\lambda = \mathscr{U}/I_\lambda$. The canonical map $\mathscr{U} \to Z_\lambda$ induces a (left) $\mathscr{N}'$-module homomorphism of $\mathscr{N}'$ *onto* Z_λ. Indeed, the coset of 1 in Z_λ is a maximal vector of weight λ. Therefore, $\dim Z_\lambda \leqslant p^m = \dim \mathscr{N}'$. Moreover, if V is any standard cyclic $\mathfrak{g}$ module of weight λ, with maximal vector v_0, then evidently $I_\lambda v_0 = 0$ and the map $\mathscr{U} \to V$ (sending 1 to v_0) is a $\mathscr{U}$-module homomorphism factoring through Z_λ.

One can also view Z_λ as an *induced module* (cf., [16]): Extend λ first to a K-linear map $\mathfrak{b} = \mathfrak{h} + \mathfrak{n} \to K$ by decreeing that $\lambda(\mathfrak{n}) = 0$. This extended λ is a restricted homomorphism of Lie algebras, since $\mathfrak{h}$ is Abelian, $[\mathfrak{h}, \mathfrak{n}] \subset \mathfrak{n}$, and $\lambda(H_i) = \lambda(H_i^p) = \lambda(H_i)^p$ [$\lambda(H_i)$, being an element of the prime field of K]. Denote by M the one-dimensional $\mathfrak{b}$ module (or $\mathscr{B}$ module) thus obtained. Next, form the induced $\mathscr{U}$ module $N = \mathscr{U} \otimes_{\mathscr{B}} M$. If m spans M, it is clear that $1 \otimes m$ is a maximal vector of weight λ in N, and that $N = \mathscr{U}(1 \otimes m)$ is standard cyclic. Therefore, N is a homomorphic image of Z_λ. On the other hand, $\mathscr{U}$ is K isomorphic to $\mathscr{N}' \otimes_K \mathscr{B}$ (by PBW), so N is K isomorphic to $\mathscr{N}' \otimes_K M$, a vector space of dimension $p^m = \dim \mathscr{N}'$. We already know that $\dim Z_\lambda \leqslant p^m$, which forces Z_λ to be isomorphic to N (as $\mathscr{U}$ modules).

PROPOSITION 1.3. *The canonical map $\mathscr{U} \to Z_\lambda$, restricted to $\mathscr{N}'$, is an isomorphism of (left) $\mathscr{N}'$ modules; in particular,* $\dim Z_\lambda = p^m$ *and* $I_\lambda \cap \mathscr{N}' = 0$.

Next we look for *minimal* vectors (nonzero vectors killed by all Y_i) in Z_λ. This information plays an essential role in Section 4.

LEMMA 1.4. *Let $(\alpha_1, \ldots, \alpha_m)$ be any ordering of the positive roots. If $ht(\alpha_k) = h$, assume that all exponents i_j in $Y_1^{i_1} \cdots Y_m^{i_m}$ for which $ht(\alpha_j) \geqslant h$ are equal to $p - 1$. Then, if Y_k is inserted anywhere into this expression, the result is* 0.

Proof. Use downward induction on h. For maximal h, Y_k commutes with everything, so we can combine it with the term Y_k^{p-1} (assumed to be present) to produce 0. In general, we have to commutate in order to move Y_k toward Y_k^{p-1}. At each step a new monomial might be introduced, with $cY_t = [Y_s, Y_k]$ replacing an occurrence of Y_s. This new monomial is obtained from one of

our standard ones by the insertion of Y_t (disregarding scalar multiples), and clearly $ht(\alpha_t) > ht(\alpha_k), ht(\alpha_s)$. It is still true that exponents are $p-1$ for roots of height at least $ht(\alpha_t)$, since the only exponent we have reduced is that of Y_s. So the induction hypothesis implies that our new monomial is 0, and therefore Y_k may finally be combined with Y_k^{p-1} to produce 0. Q.E.D.

PROPOSITION 1.5. *Up to scalar multiples, Z_λ has a unique minimal vector, the coset of $Y_1^{p-1} \cdots Y_m^{p-1}$, where $(\alpha_1, ..., \alpha_m)$ is any ordering of the positive roots.*

Proof. Lemma 1.4 shows that the coset of $Y_1^{p-1} \cdots Y_m^{p-1}$ is a minimal vector of Z_λ. (This is of course not the 0 coset, thanks to Proposition 1.3.) Now fix an order $(\alpha_1, ..., \alpha_m)$ compatible with decreasing height, and suppose $Y \in \mathcal{N}'$ represents a minimal vector of Z_λ: This means all $Y_i Y = 0$, in view of Proposition 1.3. Write Y as linear combination of distinct (hence, linearly independent) monomials $Y_1^{i_1} \cdots Y_m^{i_m}$ (exponents between 0 and $p-1$). Evidently, the condition $Y_1 Y = 0$ forces the various exponents i_1 occurring in the components of Y to be equal to $p-1$. Proceed inductively, with $j = 1, 2, ...$ to show that all $i_j = p-1$. To compute $Y_j Y$ we must move Y_j past $Y_1^{p-1} \cdots Y_{j-1}^{p-1}$ (assumed inductively to be at the beginning of each component of Y). At each step we may have to introduce a new summand, in which some $Y_i (i < j)$ is replaced by a multiple of $[Y_j, Y_i]$; but the latter insertion produces 0, as in Lemma 1.4, so Y_j may in fact be moved to its correct position without introducing any new summands. Evidently all exponents of Y_j are now forced to be $p-1$, just as in the first step of the induction. We conclude, finally, that Y must have been a scalar multiple of $Y_1^{p-1} \cdots Y_m^{p-1}$. Combined with the first line of the proof, this completes the argument. Q.E.D.

Remark. There is a more sophisticated way to prove the uniqueness assertion in the Proposition 1.5, using the fact that $\mathcal{N}'$ is a Frobenius algebra. It is easy to see (cf., Section 4 below) that $\mathcal{N}'$ is indecomposable as left $\mathcal{N}'$-module. It follows then from Ref. [7, (58.12)] that the left $\mathcal{N}'$-module $\mathcal{N}'$ has a unique irreducible submodule, which is clearly 1 dimensional. We remark also that the proof of Lemma 1.4 is similar in spirit to arguments in Refs. [11] and [6, I.2.1]. Finally, we observe that the uniqueness assertion in 1.5 provides an independent proof that Z_λ is indecomposable (not using Proposition 1.2).

Now we introduce certain *characters* analogous to those of Harish–Chandra [12, exposés 18, 19]. Let $\mathcal{C}$ be the center of $\mathcal{U}$. Since Z_λ is indecomposable and K is algebraically closed, Fitting's Lemma implies that each element of $\mathcal{C}$ acts as a scalar plus a nilpotent; since $\mathcal{C}$ is commutative, the function $\chi_\lambda : \mathcal{C} \to K$ assigning to C its single eigenvalue on Z_λ is a homomorphism of

K algebras. Moreover, $\chi_\lambda(C)$ is the single eigenvalue of C on any subhomomorphic image of Z_λ, from which we deduce:

PROPOSITION 1.6. *$\chi_\lambda = \chi_\mu$ if M_λ and M_μ occur as composition factors of some standard cyclic $\mathfrak{g}$ module.*

2. Linked Weights and Blocks

DEFINITION. Let W be the Weyl group of $\mathfrak{g}_\mathbf{C}$, ρ = halfsum of positive roots. If $\lambda, \mu \in \Lambda$, viewed as functions on $\mathfrak{h}$, satisfy: $\lambda + \rho = (\mu + \rho)^\sigma$ for some $\sigma \in W$, then we say λ and μ are *linked* and write $\lambda \sim \mu$.

It is clear that linkage is an equivalence relation on Λ, since $(\lambda_\sigma)_\tau = \lambda_{\sigma\tau}$, where we write $\lambda_\sigma = (\lambda + \rho)^\sigma - \rho$. There is always a linkage class having only one member: Take $\lambda = (p-1)\rho$; this weight yields the "Steinberg module" $M_\lambda = \bar{V}_\lambda = Z_\lambda$, the unique irreducible $\mathfrak{g}$ module of maximal dimension p^m [14, Section 8]. The condition $\lambda \sim \mu$ is analogous to Harish-Chandra's condition for equality of "characters" in the infinite-dimensional case [12, 19-09].

Assume the notation chosen so that $X_1, \ldots, X_l$ and $Y_1, \ldots, Y_l$ correspond to $\pm\Pi$. The following formulas are to be verified by induction on $n \geq 0$ in the universal enveloping algebra of $\mathfrak{g}_\mathbf{C}$ [16, Section 3]:

$$[X_j, Y_i^{n+1}] = 0, \qquad 0 \leq i \neq j \leq l,$$

$$[X_i, Y_i^{n+1}] = -(n+1)Y_i^n(n \cdot 1 - H_i), \qquad 0 \leq i \leq l,$$

$$[H_j, Y_i^{n+1}] = -(n+1)\alpha_i(H_j)Y_i^{n+1}, \qquad 0 \leq i, j \leq l.$$

The first formula follows from the fact that $\alpha_j - \alpha_i$ is not a root. For the second, write

$$\begin{aligned}[X_i, Y_i^{n+1}] &= X_iY_i^{n+1} - Y_iX_iY_i^n + Y_iX_iY_i^n - Y_i^{n+1}X_i \\ &= [X_i, Y_i]Y_i^n + Y[X_i, Y_i^n] = H_iY_i^n + Y[X_i, Y_i^n],\end{aligned}$$

then use induction and the fact that the third formula holds for n in place of $n+1$. The third formula itself follows from an obvious induction.

These formulas hold equally well in $\hat{\mathscr{U}}$, and even in $\mathscr{U}$ (where both sides always vanish when n is at least $p-1$). In particular, if $\lambda \in \Lambda$, set $n = \lambda(H_i)$, viewed as an integer between 0 and $p-1$. Then two possibilities arise: (i) $n = p-1$, so $Y_i^{n+1} = 0$ in $\mathscr{U}$; (ii) $n < p-1$, so $Y_i^{n+1} \neq 0$ and the

corresponding coset in Z_λ is a maximal vector of weight $\lambda - (n+1)\alpha_i$. To see this, use the three formulas above, and notice that the right-hand side of the third formula is congruent (mod I_λ) to $(\lambda(H_j) - (n+1)\alpha_i(H_j))Y_i^{n+1}$. But when $\sigma = \sigma_i$ is reflection relative to the *simple* root α_i, then $\lambda_\sigma = \lambda - (\lambda(H_i)+1)\alpha_i$, since σ_i permutes the positive roots other than α_i. In case (i), $\lambda_\sigma = \lambda$ and we get nothing new; in case (ii), we have produced a maximal vector of a new weight linked to λ, hence a composition factor M_{λ_σ}. We conclude that if λ and μ are linked by a simple reflection, then M_λ and M_μ occur as composition factors in both Z_λ and Z_μ. Transitivity of linkage allows us to state (using Proposition 1.6):

THEOREM 2.1. *$\lambda \sim \mu$ implies $\chi_\lambda = \chi_\mu$.*

Remark. The above procedure for constructing maximal vectors in Z_λ can be iterated to some extent, because each such maximal vector yields a homomorphism $Z_\mu \to Z_\lambda$ ($\mu = \lambda_\sigma$) under which maximal vectors in Z_μ will be sent to (possibly new) maximal vectors in Z_λ (or to 0). To be more precise, let J_λ be the left ideal in $\mathscr{U}$ generated by I_λ along with all $Y_i^{\lambda(H_i)+1}$, $1 \leqslant i \leqslant l$, and set $Z_\lambda' = \mathscr{U}/J_\lambda$. Clearly, we have epimorphisms $Z_\lambda \to Z_\lambda' \to \bar{V}_\lambda \to M_\lambda$. (Examples in A_2 show already that these objects are in general distinct; cf., Section 7 below.) If we are in case (i) above, we set $Z_\lambda(i) = 0$; in case (ii), we let $Z_\lambda(i)$ be the homomorphic image of $Z_\mu(\mu = \lambda_{\sigma_i})$ in Z_λ, constructed by sending the coset of 1 in Z_μ to the maximal vector = coset of $Y_i^{\lambda(H_i)+1}$ in Z_λ. Then $Z_\lambda/\sum_i Z_\lambda(i)$ is simply Z_λ'. The argument can be iterated within each nonzero $Z_\lambda(i)$, but further subquotients may be smaller than Z_μ' for the weight μ involved; therefore, it does not seem reasonable to expect a complete description of the submodules of Z_λ to arise from this procedure.

THEOREM 2.2. *$\lambda \sim \mu$ implies that Z_λ and Z_μ have the same composition factors (multiplicities included); in particular, M_μ is a composition factor of Z_λ.*

Proof. By transitivity of linkage, it suffices to prove this for λ and $\mu = \lambda_{\sigma_i} (\neq \lambda)$. As in the preceding Remark, we have canonical maps $\phi : Z_\mu \to Z_\lambda(i) \subset Z_\lambda$ and $\psi : Z_\lambda \to Z_\mu(i) \subset Z_\mu$. If we identify elements of Z_λ and Z_μ with their coset representatives in $\mathscr{N}^-$, then clearly ϕ and ψ are induced by *right* multiplication by Y_i^{n+1} and $Y_i^{p-(n+1)}$, respectively, where $n = \lambda(H_i)$ and $p = n - 2 = \mu(H_i)$ ($\mu = \lambda - (n+1)\alpha_i$). Therefore, $\psi \circ \phi = 0$ and $\operatorname{Im}\phi \subset \ker\psi$. Conversely, we claim that $\ker\psi \subset \operatorname{Im}\phi$. By renumbering the simple roots, we may assume $i = 1$. Then it is clear that $\ker\psi$ is spanned by the cosets of the monomials $Y_m^{i_m} \cdots Y_1^{i_1}$, where $i_1 \geqslant n+1$. This is, however, obviously a basis for $\operatorname{Im}\phi$ as well. By symmetry, we have also proved that $\ker\phi = \operatorname{Im}\psi$. Now the composition factors of Z_λ are those of $\operatorname{Im}\phi$ along with those of $Z_\lambda/\operatorname{Im}\phi = Z_\lambda/\ker\psi \approx \operatorname{Im}\psi$; similarly, the composition factors

of Z_μ are those of $\operatorname{Im}\psi$ along with those of $Z_\mu/\operatorname{Im}\psi = Z_\mu/\ker\phi \approx \operatorname{Im}\phi$. So the theorem is proved. Q.E.D.

The linkage class of λ is in 1-to-1 correspondence with the W orbit of $\lambda + \rho$ in Λ, so Theorem 2.1 shows there are no more characters than orbits. We can relate this to the *blocks* of $\mathscr{U}$ as well [7, Section 55]. The distinct (left) *principal indecomposable modules* (PIM's) of $\mathscr{U}$ correspond 1-to-1 with the elements of $\mathscr{M}$; namely, the PIM U_λ has unique highest composition factor M_λ. Two PIM's are said to be "linked" if they share a composition factor, and the sum of all PIM's in a class of this equivalence relation is an indecomposable two-sided ideal of $\mathscr{U}$, called a "block". Now let B_λ be the block containing U_λ. Since Z_λ has a unique maximal submodule, by Proposition 1.2, it is clear that (under the canonical map $\mathscr{U} \to Z_\lambda$) some copy of U_λ maps *onto* Z_λ, whence every composition factor of Z_λ belongs to the block B_λ. In view of Theorem 2.2, we can state:

THEOREM 2.3. *$\lambda \sim \mu$ implies U_λ and U_μ are linked, so $B_\lambda = B_\mu$.*

This shows that the number of distinct blocks, say t, does not exceed the number of W orbits in Λ (and each block corresponds to a union of such orbits). By general principles (cf., [7, Section 85]), t is equal to $\dim(\mathscr{C}/\operatorname{rad}\mathscr{C})$, and the blocks are distinguished from one another by the t distinct K algebra homomorphisms $\mathscr{C} \to K$ defined by block idempotents (cf. Section 0). These homomorphisms simply record the eigenvalues of elements of $\mathscr{C}$ on the various irreducible $\mathscr{U}$ modules belonging to the respective blocks, so, in particular, the homomorphism defined by the block idempotent of B_λ is χ_λ. We conclude that $\chi_\lambda = \chi_\mu$ precisely when the linkage classes of λ and μ belong to the same block. If we could show that t equals the number of linkage classes (or W orbits in Λ), then it would follow that $\chi_\lambda = \chi_\mu$ implies $\lambda \sim \mu$. The next section is devoted to this question.

3. INVARIANTS

We would like to prove the converse of Theorem 2.1. However, our method breaks down when p is "small," so we can only state the following partial converse.

THEOREM 3.1. *If $p >$ Coxeter number of Σ, then $\chi_\lambda = \chi_\mu$ implies $\lambda \sim \mu$.*

Remark. The Coxeter number h (= order of the product of all simple reflections in W) for each of the simple types is as follows [2, pp. 250–275]: A_l, $l+1$; B_l or C_l, $2l$; D_l, $2l-2$; E_6, 12; E_7, 18; E_8, 30; F_4, 12; G_2, 6.

Whenever $p > h$, p does not divide the order of W [2, Chap. V, Section 6.2].

Before proving Theorem 3.1 we must examine more closely the value of χ_λ at a central element. There is a natural K-linear map β:

$$\mathscr{U} \approx \mathscr{N}' \otimes \mathscr{H} \otimes \mathscr{N} \to \mathscr{H}$$

defined by $\beta(YHX) = 0$ if either Y or X is not 1, $\beta(YHX) = H$ if $Y = X = 1$ ($Y \in \mathscr{N}'$, $H \in \mathscr{H}$, $X \in \mathscr{N}$ standard basis monomials). Compare [12, 18–05] for the analogous map in characteristic 0, which we denote β_C; it is clear that $\hat{\beta} : \hat{\mathscr{U}} \to \hat{\mathscr{H}}$ can be defined similarly. If $\lambda \in \Lambda$ is viewed (canonically) as a K-algebra homomorphism $\mathscr{H} \to K$, then from the very definition of χ_λ we obtain: $\chi_\lambda(C) = \lambda(\beta(C))$ for $C \in \mathscr{C}$. Indeed, the scalar $\chi_\lambda(C)$ is just the coefficient of a maximal vector v generating Z_λ in the expression of Cv relative to a suitable basis whose first element is v. We observe, moreover, that $\beta \mid \mathscr{C}$ *is multiplicative*: $\lambda(\beta(CC')) = \chi_\lambda(CC') = \chi_\lambda(C)\chi_\lambda(C') = \lambda(\beta(C))\lambda(\beta(C')) = \lambda(\beta(C)\beta(C'))$, whence

$$\beta(CC') - \beta(C)\beta(C') \in \bigcap_{\lambda \in \Lambda} \ker \lambda.$$

But this intersection is rad $\mathscr{H}$ = intersection of all maximal ideals of $\mathscr{H}$, because each K-algebra homomorphism $\mathscr{H} \to K$ (or maximal ideal of $\mathscr{H}$) comes from a restricted Lie algebra representation $\mathfrak{h} \to K$, i.e., from some element of Λ. Finally, rad $\mathscr{H} = 0$ because each $H_i^p = H_i$ ($\mathscr{H}$ has no nonzero nilpotents).

The linear map $\mathfrak{h} \to \mathscr{H}$ defined by $H_i \to H_i - \rho(H_i) \cdot 1$ (ρ as before) is clearly a restricted homomorphism of $\mathfrak{h}$, because all $\rho(H_i)$ lie in the prime field of K. Therefore, it yields a K-algebra homomorphism $\gamma : \mathscr{H} \to \mathscr{H}$. Similarly, we get $\gamma' : \mathscr{H} \to \mathscr{H}$ sending H_i to $H_i + \rho(H_i) \cdot 1$, and the two composites are the identity. Therefore, γ is an automorphism of $\mathscr{H}$. It is clear that an analogous map $\hat{\gamma}$ can be defined on $\hat{\mathscr{H}}$. Write δ and $\hat{\delta}$ for the respective composites $\gamma \circ \beta$, $\hat{\gamma} \circ \hat{\beta}$. It is convenient to record here the following fact, which is obvious if we use a PBW basis for each of $\hat{\mathscr{U}}$, $\mathscr{U}$ built from the Chevalley basis.

LEMMA 3.2. *Let $r : \hat{\mathscr{U}} \to \mathscr{U}$ be the canonical map. The following diagram commutes*:

$$\begin{array}{ccc} \hat{\mathscr{U}} & \xrightarrow{\hat{\delta}} & \hat{\mathscr{H}} \\ {\scriptstyle r}\downarrow & & \downarrow{\scriptstyle r} \\ \mathscr{U} & \xrightarrow[\delta]{} & \mathscr{H} \end{array}$$

According to Theorem 2.1, $\lambda \sim \mu$ implies $\chi_\lambda = \chi_\mu$. By the previous remarks, this in turn implies that $\lambda(\beta(C)) = \mu(\beta(C))$, hence that

$$(\lambda + \rho)(\gamma(\beta(C))) = (\mu + \rho)(\gamma(\beta(C))), \qquad \text{for all} \quad C \in \mathscr{C}.$$

In other words, since each $\nu \in \Lambda$ has the form $\lambda + \rho$ for some $\lambda \in \Lambda$, all W conjugates of an arbitrary ν agree on $\delta(\mathscr{C})$. This means that each ν is constant on the W orbit of every element $\delta(C)$. Now $\mathscr{H}$ is a p^l-dimensional commutative, semisimple associative algebra over the algebraically closed field K, hence is characterized by the p^l distinct K-algebra homomorphisms $\mathscr{H} \to K$ provided by the elements of Λ, i.e., the $\nu \in \Lambda$ separate points of $\mathscr{H}$. We conclude that $\delta(\mathscr{C}) \subset \mathscr{H}^W$ (= algebra of W invariants in $\mathscr{H}$).

Let t' denote the dimension of the semisimple algebra $\mathscr{H}^W$. It is clear that the primitive idempotents here are just the sums over the various W orbits of primitive idempotents in $\mathscr{H}$. But W permutes the latter as it permutes the corresponding K-algebra homomorphisms $\mathscr{H} \to K$, i.e., as it permutes Λ. We see from this that t' = number of W orbits in Λ.

Observe next that $\ker(\beta \mid \mathscr{C}) = \operatorname{rad} \mathscr{C}$. One inclusion is obvious. If $C \in \mathscr{C} - \operatorname{rad} \mathscr{C}$, then C does not act trivially on every irreducible $\mathscr{U}$ module (i.e., C nonnilpotent implies $C \notin \operatorname{rad} \mathscr{U}$); hence $\chi_\lambda(C) \neq 0$ for some λ. But we saw that $\chi_\lambda(C) = \lambda(\beta(C))$, whence $\beta(C) \neq 0$. It follows also that $\ker(\delta \mid \mathscr{C}) = \operatorname{rad} \mathscr{C}$, whence $t = \dim \mathscr{C}/\operatorname{rad} \mathscr{C}$ (= number of blocks of $\mathscr{U}$) $\leqslant \dim \mathscr{H}^W = t'$ (= number of W orbits in Λ). In view of the final remarks in Section 2, *to prove Theorem* 3.1 *it will suffice to show that* $t = t'$, *or equivalently, that* $\delta(\mathscr{C}) = \mathscr{H}^W$.

We proceed to a closer study of $\mathscr{H}^W$. For this, some comparisons must be made with the ordinary universal enveloping algebras. As before, let $r : \hat{\mathscr{U}} \to \mathscr{U}$ be the canonical map.

LEMMA 3.3. *When* p *does not divide* $|W|$ (e.g., *when* $p > h$), $r : \hat{\mathscr{H}} \to \mathscr{H}$ *is a* W *homomorphism sending* $\hat{\mathscr{H}}^W$ *onto* $\mathscr{H}^W$.

Proof. We recall that $\ker(r \mid \hat{\mathscr{H}})$ is the two-sided ideal generated by all $H_i^p - H_i$, $1 \leqslant i \leqslant l$. Now the simple reflection σ_j sends H_i to $H_i - [2(\alpha_i, \alpha_j)/(\alpha_j, \alpha_j)]H_j$, and since the integer coefficient here is equal to its pth power in the prime field of K, we deduce that $\ker(r \mid \hat{\mathscr{H}})$ is W stable, i.e., $r : \hat{\mathscr{H}} \to \mathscr{H}$ is a W homomorphism. This implies that $r(\hat{\mathscr{H}}^W) \subset \mathscr{H}^W$. Conversely, since p does not divide $|W|$, a standard argument based on complete reducibility [9, Lemma 5.1.A] shows that invariants in $\mathscr{H}$ may be lifted to invariants in $\hat{\mathscr{H}}$.

Remark. The proof of Lemma 3.3 can also be carried through when p does divide the order of W, using a "semireductivity" technique of Nagata

[9, Lemma 5.1.B] along with the special fact that $H_i^p = H_i$. But we do not need this here. We remark also that A. Borel has proved some closely related facts about invariants of W.[3]

If R is any PID in which $|W|$ is invertible, it is wellknown that the W invariants in the polynomial algebra $R[H_1, \ldots, H_l]$ again form a polynomial algebra in l variables, with minimal homogeneous generating set of uniquely determined degrees $k_1, \ldots, k_l$ (the largest of these being the Coxeter number of W) [2, Chap. V, Sections 5.3 and 5, exercise 2]. In particular, let R be the ring of rational numbers whose denominators are relatively prime to p, so that $R/pR \approx \mathbf{F}_p$ (the field of p elements). The canonical map $R[H_1, \ldots, H_l] \to \mathbf{F}_p[H_1, \ldots, H_l]$ is a surjective W homomorphism, clearly, and the assumption $p > h$ (or just $p \nmid |W|$) shows as in the proof of Lemma 3.3 that the ring of W-invariants maps *onto* the W invariants of $\mathbf{F}_p[H_1, \ldots, H_l]$. In turn the latter generate the ring of W invariants in $\hat{\mathscr{H}}$, since invariants are preserved under base field extension. Finally, Lemma 3.3 shows that these in turn map onto $\mathscr{H}^W$. We conclude that *$\mathscr{H}^W$ is generated by its elements of degree less than p*, and to prove Theorem 3.1 it will suffice to show that these may be "lifted" to elements of $\mathscr{C}$, relative to δ. This we propose to do by going back to characteristic 0.

Let $\mathscr{U}_R$ and $\mathscr{H}_R$ be respective universal enveloping algebras of the R spans in $\mathfrak{g}_\mathbf{C}$ of the full Chevalley basis, resp. of the H_i. Clearly, $\mathscr{H}_R$ is just the polynomial algebra $R[H_1, \ldots, H_l]$ which appeared above. From elementary principles,[4] we see that $(\mathscr{U}_R \otimes_R R/pR) \otimes_{F_p} K$ is isomorphic to $\hat{\mathscr{U}}$, and similarly for the subalgebra $\mathscr{H}_R$, whence we obtain "reduction mod p" maps $\mathscr{U}_R \to \hat{\mathscr{U}}$ and $\mathscr{H}_R \to \hat{\mathscr{H}}$, to be denoted by s. One defines δ_R by analogy with the earlier maps of $\hat{\mathscr{U}}$ and $\mathscr{U}$. Then the following lemma is proved in the same manner as Lemma 3.2.

LEMMA 3.4. *The following diagram commutes:*

$$\begin{array}{ccc} \mathscr{U}_R & \xrightarrow{\delta_R} & \mathscr{H}_R \\ {\scriptstyle s}\downarrow & & \downarrow{\scriptstyle s}. \\ \hat{\mathscr{U}} & \xrightarrow{\delta} & \hat{\mathscr{H}} \end{array}$$

Now we can exploit some known facts about lifting invariants in characteristic 0. First, we recall Steinberg's proof of a result of Chevalley, which is reproduced in [16, Appendix A]. The object is to lift W-invariant polynomial

[3] A. BOREL, "Sur la torsion des groupes de Lie," *J. Math. Pures Appl.* (9) **35** (1956) 127–139, Lemma 2.3 and Theorem 2.4.

[4] See N. BOURBAKI, "Groupes et algèbres de Lie," Chap. I, Section 2, No. 9, Hermann, Paris, 1960.

functions on $\mathfrak{h}_{\mathbf{C}}$ to $G_{\mathbf{C}}$-invariant polynomial functions on $\mathfrak{g}_{\mathbf{C}}$ ($G_{\mathbf{C}}$ being a Chevalley group over $\mathbf{C}$ constructed from our Chevalley basis of $\mathfrak{g}_{\mathbf{C}}$). The polynomial functions on $\mathfrak{h}_{\mathbf{C}}$ are polynomials in the fundamental dominant weights $\lambda_1, \ldots, \lambda_l$; moreover, the powers λ^k of *all* weights λ suffice to span the algebra $\mathscr{P}(\mathfrak{h}_{\mathbf{C}})$ of polynomial functions, by polarization (see below). If sym λ^k denotes the sum of the *distinct* images of λ^k under W, then these elements span $\mathscr{P}(\mathfrak{h}_{\mathbf{C}})^W$; indeed, it suffices for this to let λ run through just the *dominant* weights. Now use induction, relative to the usual partial order on dominant weights, for a fixed integer $k > 0$, to show that sym λ^k is liftable: Suppose this is known for all dominant weights lower than λ. Take π to be the representation of $\mathfrak{g}_{\mathbf{C}}$ having highest weight λ, and set $m_\pi(\mu) =$ multiplicity of the weight μ in π. Then, $\mathrm{Tr}(\pi(X)^k)$, $X \in \mathfrak{g}_{\mathbf{C}}$ is a $G_{\mathbf{C}}$-invariant polynomial function on $\mathfrak{g}_{\mathbf{C}}$, whose restriction to $\mathfrak{h}_{\mathbf{C}}$ is

$$\sum_{\mu} m_\pi(\mu)\mu^k = \sum_{\mu \text{dominant}} m_\pi(\mu)\ \mathrm{sym}\ \mu^k,$$

multiplicity being constant on W orbits. The right side differs from sym λ^k by a W-invariant polynomial already known (by induction) to be liftable, so we're done.

Two comments must be made. First, if we use an admissible lattice in the representation space of π, the trace occurring in Steinberg's proof will be a $\mathbf{Z}$ polynomial in the linear functions dual to the Chevalley basis. Second, the process of polarization mentioned above entails expressing monomials of total degree k in $\lambda_1, \ldots, \lambda_l$ as linear combinations of pure kth powers of various linear combinations of the λ_i. This can all be done over $\mathbf{Z}$, except for denominators divisible by primes less than k, hence can all be done over the ring R if we are only concerned with lifting invariants of degree less than p.

Relative to the Killing form on $\mathfrak{g}_{\mathbf{C}}$, one can realize the dual basis $\{X^*, H_i^*\}$ within $\mathfrak{g}_{\mathbf{C}}$ itself; for example, in type A_1 we have the identifications $X^* = \frac{1}{4}Y$, $H^* = \frac{1}{8}H$, $Y^* = \frac{1}{4}X$. In general, the donominators involved in expressing the dual basis in terms of the Chevalley basis involve nothing but factors of the discriminant of the Killing form; but the latter are all prime to p by our restriction $p > h$ (cf., G. B. Seligman, "Modular Lie Algebras," p. 47, Springer-Verlag, Berlin, 1967).

In the standard argument in characteristic 0 (cf., [16, Appendix A]), one starts with a W-invariant element of $\mathscr{H}_{\mathbf{C}}$, passes to an element of $\mathscr{P}(\mathfrak{h}_{\mathbf{C}})^W$ by going over to the dual basis, then lifts to a $G_{\mathbf{C}}$-invariant polynomial on $\mathfrak{g}_{\mathbf{C}}$ using Chevalley's theorem above; the next step is to pass back to the Chevalley basis, writing a polynomial function first as a (commuting) tensor in terms of the dual basis, then replacing this with the corresponding tensor in terms of the Chevalley basis; the latter is no longer commuting, so one has to

symmetrize and then map the result (canonically) into $\mathscr{U}_{\mathbf{C}}$.[5] The algorithm just described is implicit in the discussion of [12, exposé 19], but is not emphasized there. In view of our preceding remarks, there is no special difficulty in carrying out the whole process over R, if we only wish to lift invariants of degrees less than p. (The symmetrization only requires denominators of the form $k!$, where k is the degree.) We conclude that for each element of $\mathscr{H}_R{}^W$, there is a central element of $\mathscr{U}_R$ mapping back to the given element under δ_R. Being central in $\mathscr{U}_R$ just means commuting with the Chevalley basis, and this property is evidently preserved under the "reduction mod p" map s, then under r. Combining this with Lemmas 3.2 and 3.4, we see finally that a generating set for $\mathscr{H}^W$ lifts (relative to δ) to a subset of $\mathscr{C}$, thus completing the proof of Theorem 3.1.

Remark. A closer examination of some of the above steps shows that, under the assumption $p > h$, one can do Steinberg's proof of Chevalley's theorem directly in characteristic p. Namely, observe that W-invariant polynomials of degree less than p are adequate to generate the rest, then observe that these in turn can all be gotten (by polarization) from those of the form sym (λ^k), and then lift the latter explicitly by constructing the appropriate traces. Therefore, $\mathscr{P}(\mathfrak{g})^G \to \mathscr{P}(\mathfrak{h})^W$ (which is always 1-to-1) is onto in this case. If $\mathfrak{g}$ is taken to be the Lie algebra of an *adjoint* group, it can be proved uniformly for *arbitrary* characteristic that the analogous map is onto.[6] This proof actually goes through for $p \neq 2$ for our algebra $\mathfrak{g}$.

EXAMPLE. Our proof via char 0 is awkward; one would like to find a more intrinsic method which might relax the restriction on p. Nonetheless, our method here is constructive in nature, as the following example illustrates.

Consider the algebra $\mathfrak{g} = sl(2, K)$ of type A_1, with the usual Chevalley basis (X, H, Y). Assume $p \neq 2$. As a generator of $\hat{\mathscr{H}}^W$ (or of $\mathscr{H}^W$) we may take H^2 (which also works when $p = 2$). If λ is the fundamental dominant weight, then $\lambda = H^*$; we have to see how the polynomial λ^2 lifts. λ being the highest weight of the usual representation π of $\mathfrak{g}$, we compute

$$\operatorname{Tr}\begin{pmatrix} b & a \\ c & -b \end{pmatrix}^2 = \operatorname{Tr}(\pi(aX + bH + cY))^2$$
$$= 2(H^{*2} + X^*Y^*)\begin{pmatrix} b & a \\ c & -b \end{pmatrix}.$$

Notice that a factor of 2 enters into the calculation. In this particularly simple situation, we see that the polynomial $H^{*2} + X^*Y^*$, when restricted to $\mathscr{H}$,

[5] For this last step, cf., *Ibid.* (footnote 4), Section 2, No. 5.

[6] See T. A. SPRINGER and R. STEINBERG, Conjugacy classes, in "Seminar on Algebraic Groups and Related Finite Groups," Lecture Notes in Math. No. 131, Springer–Verlag, Berlin, 1970 (II, 3.17).

already yields (without resort to induction) the W-invariant polynomial $H^{*2}(=\lambda^2)$ on $\mathfrak{h}$. Next we rewrite the polynomial as a tensor

$$H^* \otimes H^* + X^* \otimes Y^*,$$

symmetrize to $(H^* \otimes H^*) + \frac{1}{2}(X^* \otimes Y^* + Y^* \otimes X^*)$, and then revert to the Chevalley basis before mapping into $\mathscr{U}$. The upshot is that we get $H^2 + 2H + 4YX$, a "Casimir element" in $\mathscr{C}$ which maps to $H^2 + 2H$ under β, then to $H^2 - 1$ under γ. The lifting process may be summarized as follows:

$$\begin{aligned} H^2 &\to 64H^{*2} \to 64(H^{*2} + X^*Y^*) \\ &\to 64(H^* \otimes H^*) + 64/2(X^* \otimes Y^* + Y^* \otimes X^*) \\ &\to (H \otimes H) + 2(Y \otimes X + X \otimes Y) \\ &\to H^2 + 2YX + 2XY = H^2 + 2H + 4YX. \end{aligned}$$

4. Projective Modules

The projective $\mathscr{U}$ modules are just the direct sums of the PIM's (which are the only indecomposable projectives) [7, Section 56]. It is clear that if M is indecomposable and $P \to M \to 0$ is a projective cover, then a sum of PIM'S from the *same* block already maps onto M. Since every $\mathscr{U}$ module has a projective cover, we deduce from Theorems 2.3 and 3.1:

Theorem 4.1. *If $p >$ Coxeter number of W, then if M is an indecomposable $\mathscr{U}$ module, all composition factors of M have highest weights which are linked.*

This has been conjectured (with no special restriction on p) for the corresponding algebraic group G by Verma; in Section 5 below we shall see how to obtain that result from Theorem 4.1. Pollack's study of type A_1 confirms Theorem 4.1 directly [10], and Braden's conclusions [3, 4] are highly consistent with it. (The restrictions placed on p by Pollack and Braden amount to the hypothesis $p > h$.) In view of Theorem 2.2, the conclusion of 4.1 is "best possible."

In the rest of this section we shall be concerned with describing more explicitly the PIM's of $\mathscr{U}$. The results we obtain generalize Pollack's theorems for A_1 [10]. As an auxiliary tool we determine the projective modules for $\mathscr{N}$ (or $\mathscr{N}'$) and for the subalgebra $\mathscr{B}'$ of $\mathscr{U}$ generated by $\mathscr{H}$ and $\mathscr{N}'$ ($\mathscr{B}'$ is the u algebra of $\mathfrak{h} + \mathfrak{n}'$). Then we combine this information with earlier facts about the standard cyclic modules Z_λ.

Proposition 4.2. *Projective $\mathscr{N}$ modules are free (so $\mathscr{N}$ is its own unique*

PIM). *Moreover, every projective $\mathscr{U}$ module is projective as $\mathscr{N}$ module; in particular, each* PIM *of $\mathscr{U}$ has dimension divisible by $p^m = \dim \mathscr{N}$ (m = number of positive roots).*

Proof. $\mathscr{N}$ has a basis consisting of 1 along with the other monomials $X_1^{i_1} \cdots X_m^{i_m}$ $(0 \leqslant i_j < p)$. So $\mathscr{N}$ is a local ring, with unique maximal two-sided ideal (= radical) spanned by the latter collection of nilpotents (cf., [6, I.2.1]). It follows by a standard argument [7, p. 383, exercise 2] that every (finite-dimensional) projective $\mathscr{N}$ module is free. Now $\mathscr{U}$ is evidently a free $\mathscr{N}$ module, with $\mathscr{N}$ basis consisting of the standard basis monomials not involving $X_1, \ldots, X_m$. Therefore any PIM of $\mathscr{U}$ is projective as $\mathscr{N}$-module, hence free as $\mathscr{N}$-module by the first part of the proposition. Q.E.D.

This is analogous to a classical theorem on group algebras of finite groups [7, 65.17]. We observe that only the Steinberg module (as PIM) can have dimension as small as p^m; other PIM's are strictly larger, for reasons which will become apparent later. One other remark: If we replace $\mathscr{N}$ by $\mathscr{N}'$ in Proposition 4.2, the resulting statement is obviously true, and if in addition we replace $\mathscr{U}$ by $\mathscr{B}'$ in the second part of the proposition, we again have a true statement (the proof goes through as before).

PROPOSITION 4.3. *Every projective $\mathscr{U}$ module is also projective as $\mathscr{B}'$ module. The* PIM's *of $\mathscr{B}'$ are just the p^l distinct modules Z_λ $(\lambda \in \Lambda)$ viewed as $\mathscr{B}'$ modules, each occurring in $\mathscr{B}'$ with multiplicity one and in $\mathscr{U}$ with multiplicity p^m.*

Proof. For the first assertion, it suffices to show that $\mathscr{U}$ itself is projective as $\mathscr{B}'$ module. We shall show how to write $\mathscr{U}$ as direct sum of various $\mathscr{B}'$ modules Z_λ, and then conclude by proving the second assertion. To begin with, $\mathscr{H}$ is a commutative semisimple associative algebra (semisimple because, as noted in Section 3, $H_i^p = H_i$ rules out nilpotents). The left regular representation of $\mathscr{H}$ then decomposes into the direct sum of p^l (= $\dim \mathscr{H}$) one-dimensional representations, each given by a K-algebra homomorphism $\mathscr{H} \to K$, or equivalently, by a *restricted* representation $\mathfrak{h} \to K$. The latter is given by a linear function λ, which must satisfy $\lambda(H_i) = \lambda(H_i^p) = \lambda(H_i)^p$; in other words, $\lambda \in \Lambda$, Λ being the set of *all* linear functions on $\mathfrak{h}$ whose values at the H_i lie in the prime field of K. Let $W_1, \ldots, W_q$ $(q = p^l)$ be a basis for $\mathscr{H}$ corresponding to the above decomposition; for fixed j, the span T_j of all $Y_1^{i_1} \cdots Y_m^{i_m} W_j$, $0 \leqslant i_t < p$, is evidently a $\mathscr{B}'$ submodule of $\mathscr{B}'$, isomorphic to the $\mathscr{B}'$ module Z_λ (where λ is the linear function corresponding to W_j : $HW_j = \lambda(H)W_j$ for $H \in \mathfrak{h}$). Moreover, $\mathscr{B}'$ is obviously the direct sum of the T_j, $j = 1, \ldots, q$. Now, if we take a fixed product $X_1^{j_1} \cdots X_m^{j_m}$ and multiply T_j by it on the *right*, we get another (left) $\mathscr{B}'$ submodule of $\mathscr{U}$ isomorphic to T_j. $\mathscr{U}$ is clearly the direct sum of these $\mathscr{B}'$ submodules (each T_j being a

summand p^m times). Now, finally, the remark following Proposition 4.2 shows that each PIM of $\mathscr{B}'$ has dimension divisible by p^m, which forces the T_j to be PIM's. By a general property of Frobenius algebras [7, 61.13], each PIM of $\mathscr{B}'$ occurs as many times as the degree of its top composition factor (i.e., once), which forces all the T_j to be distinct. Since there are p^l of them, each Z_λ ($\lambda \in \Lambda$) must occur precisely once as PIM of $\mathscr{B}'$ (and p^m times in the decomposition of $\mathscr{U}$). This completes the proof.

Remark. The decomposition of the left regular representation of $\mathscr{H}$ used in the proof of 4.3 can in fact be written down explicitly, although we did not need to do so. Suitable orthogonal idempotents are constructed by G. M. Nielsen.[7]

Proposition 4.3 gives us a method for studying the PIM's U_λ of $\mathscr{U}$ (a method which seems to underlie Pollack's study of A_1). The idea is to show that the composition factors of U_λ are precisely those of the various *$\mathscr{U}$-modules* Z_μ which enter into the decomposition of U_λ *as $\mathscr{B}'$-module.* For this we shall rely heavily on the fact (Proposition 1.5) that Z_μ has a unique (up to scalars) minimal vector, viz., the coset of $Y_1^{p-1} \cdots Y_m^{p-1}$ ($Y_1, \ldots, Y_m$ taken in any fixed order). For convenience we fix the following notation: e_μ and f_μ are respectively the maximal and the minimal vector in Z_μ given by the cosets of 1, $Y_1^{p-1} \cdots Y_m^{p-1}$. If $x \in U_\lambda$ is a vector of weight μ whose annihilator in $\mathscr{N}^-$ is 0 (i.e., such that $\mathscr{N}^- x$ has dimension p^m, hence is isomorphic to the $\mathscr{N}^-$ module Z_μ), we call x *μ special.* It is enough to check whether or not $Y_1^{p-1} \cdots Y_m^{p-1} x$ is zero (by Proposition 1.5): The annihilator of x in $\mathscr{N}^-$ is a left ideal, hence (if nonzero) contains some element annihilated by all $Y \in \mathscr{N}^-$ under left multiplication. Next, write $U_\lambda = \sum_\mu b_{\lambda\mu} Z_\mu$ as $\mathscr{B}'$ module; let $c_{\lambda\mu}$ (resp. $d_{\lambda\mu}$) = multiplicity of M_μ as composition factor of U_λ (resp. Z_λ), viewed as $\mathscr{U}$ modules. Let B, C, and D be the corresponding $p^l \times p^l$ matrices of integers (C is the "Cartan matrix" of $\mathscr{U}$ [7, p. 593]).

THEOREM 4.4. $C = BD$.

Proof. This will be carried out in several steps.

Step (i). Consider a fixed $\mathscr{B}'$ summand $\mathscr{N}^- e_\mu$ of U_λ. We ask how close it comes to being a $\mathscr{U}$ submodule: Clearly the action of the X_i is crucial. *Suppose* e_μ lies in the $\mathscr{U}$ submodule of U_λ generated by all $X_i e_\mu$ ($i = 1, \ldots, m$). Then e_μ must be a K linear combination of linearly independent "monomials" of two sorts (each having weight μ):

[7] G. M. NIELSEN, "A determination of the minimal right ideals in the enveloping algebra of a Lie algebra of classical type," Dissertation, University of Wisconsin, 1963. See also R. D. POLLACK, "Restricted Lie algebras of bounded type," Dissertation, Yale University, 1967.

(I) $Y_1^{i_1} \cdots Y_m^{i_m} X_1^{j_1} \cdots X_m^{j_m} e_\mu$, not all $i_t = 0$, not all $j_t = 0$;

(II) $X_1^{j_1} \cdots X_m^{j_m} e_\mu$, not all $j_t = 0$.

By Lemma 1.4, $Y_1^{p-1} \cdots Y_m^{p-1}$ kills all terms of type (I), so applying this element of $\mathscr{N}'$ to our expression for e_μ, we see that the summand x involving terms of type (II) must be nonzero and must in fact be μ special, generating a $\mathscr{B}'$ submodule of type Z_μ whose minimal vector is again f_μ. Now x has the form Xe_μ, where $X \in \operatorname{rad} \mathscr{N}$, because the standard basis elements of $\mathscr{N}$ (other than 1) span rad $\mathscr{N}$ (cf., proof of 4.2). Consider all vectors x of the form Xe_μ ($X \in \operatorname{rad} \mathscr{N}$) which are μ special with minimal vector f_μ. We take x from this collection such that for all X' in rad $\mathscr{N}$, $X'x$ is *not* in the collection, which is possible because rad $\mathscr{N}$ is nilpotent. Then two things are clear: First, x does *not* lie in the $\mathscr{U}$ submodule M of U_λ generated by all $X_i x$, since otherwise we could carry out the preceding argument (for x) and replace it by something of the form $X'x$ for X' in rad $\mathscr{N}$. Second, no μ-special vector in M can generate a copy of Z_μ in M whose minimal vector coincides with f_μ; to see this, write such a vector as linear combination of terms of types (I) and (II), and observe that after applying $Y_1^{p-1} \cdots Y_m^{p-1}$ we would get f_μ only if the summand of type (II) were of the form $X'x$, X' in rad $\mathscr{N}$.

Step (ii). Start with an arbitrary decomposition of U_λ as direct sum of copies of various $\mathscr{B}'$-modules Z_μ. If each summand is replaced in the manner prescribed by Step (i), we claim that the resulting sum is again *direct* (hence it again spans U_λ as well). Otherwise, we could write a dependence relation, then apply elements of $\mathscr{N}'$ systematically until we are left with a nontrival dependence relation among certain minimal vectors, which by Proposition 1.5 are still the original minimal vectors, but this is absurd since the latter are linearly independent.

For later use we record here a related remark: Suppose $\mathscr{N}'e_\mu$ is one of our direct summands. If x is an arbitrary vector of weight μ, *not* μ special, then clearly $e_\mu + x$ is μ special and yields f_μ again as minimal vector (since $Y_1^{p-1} \cdots Y_m^{p-1} x = 0$). The argument above can be used to show that replacement of $\mathscr{N}'e_\mu$ by $\mathscr{N}'(e_\mu + x)$ does not disturb the directness of the sum. (We do not, however, claim that $e_\mu + x$ will have the special "maximal" character of e_μ as in the choice made in Step (i).)

Step (iii). Fix a modified decomposition of U_λ as in Step (ii), and let $\mathscr{N}'e_\mu = P$ be a typical summand. If M denotes the $\mathscr{U}$ submodule of U_λ generated by all $X_i e_\mu$, then clearly $N = M + P$ is a $\mathscr{U}$ submodule. By our choice of e_μ (Step (i)), $0 \neq N/M$ is standard cyclic of weight μ, generated by $e_\mu + M$. According to the standard criterion for multiplicity of composition factors in terms of intertwining [7, Section 54], there exists a $\mathscr{U}$-module homomorphism $\phi : U_\mu \to N$ whose composite with $\psi : N \to N/M$ has image

not contained in the (unique) maximal submodule (i.e., such that the composite map $U_\mu \xrightarrow{\phi} N \xrightarrow{\psi} N/M \xrightarrow{\text{canon}} M_\mu$ is *onto*). On the other hand, recall from Section 1 the existence of a map π from U_μ *onto* Z_μ; pick a weight vector $e \in U_\mu$ of weight μ which maps onto a generator of Z_μ under π (so, in particular, e is μ special). Evidently, for *any* $\mathscr{U}$-homomorphism $U_\mu \xrightarrow{\text{onto}} M_\mu$, e must map to a maximal vector of M_μ, since U_μ has a unique maximal submodule (and e can't be in it). This implies, in particular, that $\psi(\phi(e)) = \psi(e_\mu)$, so that $\phi(e) = e_\mu + x$ for some vector $x \in M$ (of weight μ). By the choice of e_μ (Step (i)), $y = Y_1^{p-1} \cdots Y_m^{p-1}x$ is *not* a nonzero multiple of f_μ. Therefore, $\phi(Y_1^{p-1} \cdots Y_m^{p-1}e) = Y_1^{p-1} \cdots Y_m^{p-1}\phi(e) = f_\mu + y \neq 0$; this means that $\phi(e)$ is μ special in N, whence we obtain the $\mathscr{U}$*-module* Z_μ as subhomomorphic image of U_λ. Explicitly, ϕ induces a *bijection*

$$Z_\mu \approx U_\mu/\ker \pi \to \phi(U_\mu)/\phi(\ker \pi).$$

Two cases must now be distinguished:

Case (a): x *is not* μ *special.* In this case, as remarked in Step (ii), we may replace e_μ by $e_\mu + x$ without disturbing our direct sum.

Case (b): x *is* μ *special.* Let M_1 be the $\mathscr{U}$ submodule of M generated by all $X_i x$. Suppose $x \in M_1$, and write it in the form $z_1 + x_1$ as linear combination of vectors of weight μ involving, respectively, terms of types (I) and (II) relative to x (cf., Step (i)). Evidently x_1 is μ special, while z_1 is not, and $e_\mu + x = (e_\mu + z_1) + x_1$. Now $x_1 \in M_1$, and a repetition of this procedure leads to $x_1 = z_2 + x_2$, etc. Nilpotency of rad $\mathscr{N}$ assures us that we eventually find x_t *not* belonging to the $\mathscr{U}$ submodule generated by all $X_i x_t$. Moreover, $z_1 + \cdots + z_t$ is evidently not μ special. *Changing notation*, we conclude that $e_\mu + x = (e_\mu + z_1) + x_1$, where $x_1 \in M$ is μ special but does not belong to the $\mathscr{U}$ submodule M_1 of M generated by all $X_i x_1$, and where $z_1 \in M$ is not μ special. (In particular, M_1 is properly contained in M.) Now M/M_1 is standard cyclic of weight μ, generated by $x_1 + M_1$. Accordingly, we can find a $\mathscr{U}$-module homomorphism $\phi_1 : U_\mu \to M$ with $\phi_1(e) = x_1 - x_2$ for some $x_2 \in M_1$. Thus $(\phi - \phi_1)(e) = (e_\mu + z_1) - x_2$. We now repeat the whole process, with $-x_2$ in place of x and $\phi - \phi_1$ in place of ϕ: The only change is the addition of z_1 to e_μ, which we carry along. The module M_1 in which x_2 lies is strictly smaller than the module M in which x lies; this makes it clear that we come eventually to the following situation: $\phi : U_\mu \to N$, $\phi(e) = (e_\mu + z) + x$, $z \in M$ not μ special, $x \in M$ *u* special, and all $X_i x = 0$. Now x generates a $\mathscr{U}$-submodule Q of M isomorphic to Z_μ; since Q is already standard cyclic, we use the earlier map π to obtain a $\mathscr{U}$-homomorphism $\phi' : U_\mu \to Q$ sending e to x. Finally, $(\phi - \phi')(e) = e + z$.

In either Case (a) or Case (b), we can now use the remark in Step (ii) to

replace e_μ by, respectively, $e_\mu + x$, $e_\mu + z$, without disturbing directness of sum, and the latter element is $\phi(e)$ for *suitable* $\phi : U_\mu \to N$.

Step (iv). We showed in Step (iii) how to construct, for each (revised) summand $\mathscr{N}'e_\mu$, a homomorphism of a submodule of U_λ onto Z_μ which maps $\mathscr{N}'e_\mu$ 1-1 onto Z_μ. Referring again to the multiplicity criterion in terms of intertwining numbers, we see that each composition factor of U_λ gets accounted for in one of these subhomomorphic images Z_μ (and it gets counted the right number of times, due to the directness of our $\mathscr{B}'$ module decomposition, which assures linear independence over K of the various maps $U_\mu \to U_\lambda$ one needs to consider). This shows that $C = BD$, as required. Q.E.D.

In order to obtain precise information about dimensions, we need to *assume now that the conclusion of Theorem* 4.1 *holds.* It is clear that $\mathrm{Tr}(ad\, X) = 0$ for all $X \in \mathfrak{g}$ (look at the Chevalley basis); so Schue's theorem [11] says that $\mathscr{U}$ is a *symmetric* algebra, which in turn implies that C is a symmetric matrix.[8] Now let $\dim U_\lambda = n_\lambda p^m$. Because of Theorem 4.1 (along with Theorem 4.4), the n_λ $\mathscr{B}'$-summands Z_μ of U_λ satisfy $\mu \sim \lambda$. Theorem 2.2 asserts that each of these Z_μ's, as $\mathscr{U}$ module, has the same composition factors, or in other words, $d_{\lambda\mu} = d_{\mu\mu}$ whenever $\lambda \sim \mu$. Accordingly, $c_{\lambda\mu} = n_\lambda d_{\mu\mu}$; by symmetry of C, this also equals $n_\mu d_{\lambda\lambda}$. We conclude that for λ and μ in the same linkage class, $n_\lambda / d_{\lambda\lambda} = n_\mu / d_{\mu\mu}$ is a rational constant, to be denoted $\tilde{a}_\lambda$. The most obvious constant attached to a linkage class is its cardinality, and indeed, we shall prove that this is the value of $\tilde{a}_\lambda$.

THEOREM 4.5. *Assume that the conclusion of Theorem* 4.1 *holds. Then we have* $C = {}^tD \cdot D$, $\dim U_\lambda = a_\lambda d_{\lambda\lambda} p^m$, *and* $\dim B_\lambda = a_\lambda p^{2m}$ (a_λ = *cardinality of the linkage class of* λ).

Proof. Whenever the $\mathscr{B}'$-module Z_μ occurs as direct summand in a block B_λ of $\mathscr{U}$, we get a *minimal* vector of weight

$$\mu - (p-1)\sum_{i=1}^{m} \alpha_i = \mu + \sum_{i=1}^{m} \alpha_i = \mu + 2\rho;$$

in turn, this weight uniquely determines μ. Now, by considering minimal in place of maximal vectors (which of course requires us to replace ρ by $-\rho$), it is clear that all weights of minimal vectors occurring in a given block must be "linked"; in turn, we deduce that μ must be linked to λ. But we saw earlier (Proposition 4.3) that Z_μ occurs p^m times as a $\mathscr{B}'$ summand of $\mathscr{U}$, and since all these occurrences must be in the same block B_λ, we get $\dim B_\lambda = a_\lambda p^m p^m$,

[8] C. NESBITT, Regular representations of algebras, *Ann. Math.* **39** (1938), 634–658, Theorem 8.

a_λ being the cardinality of the class of λ. As we remarked before the statement of Theorem 4.5, dim $U_\lambda = \tilde{a}_\lambda d_{\lambda\lambda} p^m$ with $\tilde{a}_\lambda$ constant on the linkage class. $\mathscr{U}$ is Frobenius, so by general principles [7, 61.13], U_λ occurs in its block $m_\lambda = \dim M_\lambda$ times; thus the total contribution of U_λ to the dimension of B_λ is $\tilde{a}_\lambda m_\lambda d_{\lambda\lambda} p^m$. Summing over the linkage class, and using the fact that the sum of the $m_\mu d_{\lambda\mu}$ is dim $Z_\lambda = p^m$, we get dim $B_\lambda = \tilde{a}_\lambda p^m p^m$. Comparing this with the previous equation, we conclude that $\tilde{a}_\lambda = a_\lambda$ as desired. Finally, the equation $C = {}^tD \cdot D$ (or $B = {}^tD$) is an immediate consequence of Theorem 4.4, along with the above calculations.

Remark. The equation $C = {}^tD \cdot D$ resembles the well-known theorem of Brauer–Nesbitt for modular group algebras [7, 83.9], although our matrix D is not a "decomposition matrix" in the same sense as theirs. One cannot expect too strong an analogy here; for example, our matrix C has determinant 0, whereas the Cartan matrix of a modular group algebra has determinant equal to a power of p [7, 84.17]

5. Indecomposable G-Modules

In this section we shall prove the analog of Theorem 4.1 for G. Recall that G is the *simply-connected* Chevalley group of type $\mathfrak{g}_{\mathbf{C}}$; this choice of G insures that $\mathfrak{g}$ is precisely the Lie algebra of G [15, p. 64], which is not always the case when G is (say) of adjoint type. Then G has a (unique) maximal torus T whose Lie algebra is $\mathfrak{h}$, and elements of the group $X(T)$ of rational characters of T have as differentials the linear functions in Λ. The statement that G is simply-connected is equivalent to the statement that $X(T)$ is the full lattice Λ_0 of weights. For convenience, we shall regard Λ as a subset of the dominant weights in Λ_0; but when we regard $\lambda \in \Lambda_0$ as a function on $\mathfrak{h}$ we shall now write $\bar{\lambda}$, to avoid confusion. It is obvious that the theorem stated below will carry over to any smaller group in the isogeny class of G; but it should be kept in mind that, for such groups, not every dominant $\lambda \in \Lambda_0$ need be the highest weight of an irreducible *linear* representation (only of a *projective* one).

Let us compare weights for G and $\mathfrak{g}$. Obviously, $\bar{\lambda} = \bar{\mu}$ iff $\lambda \equiv \mu \pmod{p}$ in Λ_0. This allows us to define an equivalence relation on Λ_0 by: $\lambda \sim \mu$ iff $\bar{\lambda} \sim \bar{\mu}$ (linkage in the sense of Section 2). Now each dominant $\lambda \in \Lambda_0$ has a unique expression $\lambda = \lambda_0 + p\lambda_1 + \cdots + p^k\lambda_k$, where all $\lambda_i \in \Lambda$. It follows at once that $\lambda \sim \mu$ iff $\lambda_0 \sim \mu_0$ iff $\bar{\lambda}_0 \sim \bar{\mu}_0$.

For dominant $\lambda \in \Lambda_0$, let M_λ be the irreducible G module of highest weight λ. According to Steinberg's tensor product theorem [1, Theorem 7.5; 14, Section 5; 15, Section 12] we have M_λ isomorphic to

$$M_{\lambda_0} \otimes M_{\lambda_1}^{(p)} \otimes \cdots \otimes M_{\lambda_k}^{(p^k)},$$

where $\lambda = \lambda_0 + p\lambda_1 + \cdots + p^k\lambda_k$ as above and where the superscripts refer to a certain twisting. M_λ has as maximal vector $v = v_0 \otimes v_1 \otimes \cdots \otimes v_k$, where each v_i is maximal of weight λ_i in the irreducible G module M_{λ_i}. The tensor product construction makes it obvious that for M_λ viewed as (restricted) $\mathfrak{g}$ module, v is a maximal vector of weight $\bar{\lambda}_0$, because taking differentials kills the pth powers. Therefore, M_{λ_0} is a $\mathfrak{g}$ composition factor of M_λ.

On the other hand, any irreducible G module is automatically completely reducible as $\mathfrak{g}$ module (a fact pointed out to me by D. J. Winter): Take any irreducible $\mathfrak{g}$ submodule, then the sum of its G translates will be a G-stable submodule (hence the entire module) and at the same time will be a (direct) sum of irreducible $\mathfrak{g}$ modules. Moreover, any two of these $\mathfrak{g}$ modules must be isomorphic: this follows as in the argument of Curtis [6, pp. 317, 318], where he considers the effect of the standard unipotent generators of G (or close enough relative), using (respectively) maximal and minimal vectors in the $\mathfrak{g}$ modules. From the preceding paragraph we now conclude that M_λ as $\mathfrak{g}$ module is a direct sum of copies of M_{λ_0}.

One further connection between G and $\mathfrak{g}$ must be recalled before we reach our theorem. Elements of $\mathfrak{g}$, and hence also of $\mathscr{U}$, act as left invariant differential operators on the affine algebra $K[G]$ of G [13, Section 1], i.e., commute with left translation by elements of G. Those elements of $\mathscr{U}$ which also commute with right translations induce *invariant differential operators*. Now the adjoint representation of G on $\mathfrak{g}$ yields a rational action of G on $\mathscr{U}$ (as K-algebra automorphisms), and clearly the fixed points of $\mathscr{U}$ under G yield invariant differential operators. Moreover, since *ad* is the differential of *Ad*, it is immediate that these elements of $\mathscr{U}$ lie in $\mathscr{C}$ (although the reverse inclusion is doubtful). As a group of automorphisms of $\mathscr{U}$, hence of $\mathscr{C}$, G must permute the (uniquely determined) orthogonal idempotents (Section 0) which span the unique Wedderburn complement $\mathscr{C}_0$ to rad $\mathscr{C}$. But G is connected, and the group of such permutations is finite, hence the action of G on $\mathscr{C}_0$ must in fact be trivial. This shows that $\mathscr{C}$ contains "sufficiently many" G invariants.

THEOREM 5.1. *Assume that the conclusion of Theorem* 3.1 *holds. Then if* M *is an indecomposable (rational)* G *module, the highest weights of any two composition factors of* M *are linked in* Λ_0.

Proof. According to 3.1 and the preceding remarks, we have $\lambda \sim \mu$ iff $\bar{\lambda}_0 \sim \bar{\mu}_0$ iff $\chi_{\bar{\lambda}_0} = \chi_{\bar{\mu}_0}$. So $\lambda \not\sim \mu$ implies we can find $C \in \mathscr{C}$ at which $\chi_{\bar{\lambda}_0}$ and $\chi_{\bar{\mu}_0}$ take distinct nonzero values. From the discussion above, we see that C may be assumed to be G invariant. Now one can repeat almost verbatim the arguments of Springer [13, 3.3 and 4.5–4.8] to complete the proof, since

those arguments require only that we be able to produce a G invariant whose eigenvalues on certain modules are distinct. (Springer considered only the specific choice: C = Casimir element.)

6. Defect of a Block

One can introduce the notion of "defect" of a block B of $\mathscr{U}$ as follows (by analogy with the definition for modular group algebras): Let n = smallest integer such that p^n is the full power of p dividing dim V_λ (in which case we write p-dim $V_\lambda = n$) for $\lambda \in \Lambda$ such that M_λ belongs to B; then $d = m - n$ is called the *defect* of B. The block of the Steinberg module is the unique block of defect 0, clearly.

We can use Weyl's formula (in char 0) to investigate this notion more closely. Let Λ_0 be the full weight lattice of the (irreducible) root system Σ, as in Section 5. Then write $\langle \lambda, \alpha \rangle = 2(\lambda, \alpha)/(\alpha, \alpha)$ for $\lambda \in \Lambda_0$, $\alpha \in \Sigma$. (This is always an integer.) According to Weyl's formula,

$$\dim V_\lambda = \prod_{\alpha > 0} (\lambda + \rho, \alpha)/(\rho, \alpha) = \prod_{\alpha > 0} \langle \lambda + \rho, \alpha \rangle \Big/ \prod_{\alpha > 0} \langle \rho, \alpha \rangle,$$

where the integers in the final denominator depend only on Σ. Recall [2, p. 284] that Σ has a unique highest root $\sum_{i=1}^{l} n_i \alpha_i$, where $(\sum_i n_i) + 1 = h$ (the Coxeter number). Since $\rho = \sum_{i=1}^{l} \lambda_i$ and $\langle \lambda_i, \alpha_j \rangle = \delta_{ij}$, it follows that $0 < \langle \rho, \alpha \rangle < h$ for all $\alpha > 0$. Similarly, if $\lambda \in \Lambda$ (Λ viewed here as a subset of the dominant weights in Λ_0), then $0 < \langle \lambda + \rho, \alpha \rangle < ph$ for all $\alpha > 0$.

Proposition 6.1. *Let $p > h$ and $\lambda \in \Lambda$. Then p-dim V_λ is equal to the number of reflections in W fixing $\lambda + \rho$ (viewed as element of Λ).*

Proof. It is well known that all reflections in W are with respect to roots, and of course we need only consider positive roots. Let $\alpha > 0$; then, in Λ_0, we have

$$(\lambda + \rho)^{\sigma_\alpha} = \lambda + \rho - \langle \lambda + \rho, \alpha \rangle \alpha.$$

The assumption $p > h$ easily implies that, in Λ_0, $\alpha \not\equiv 0 \pmod{p}$ for all $\alpha \in \Sigma$.[9] Then we see that in Λ, $(\lambda + \rho)^{\sigma_\alpha} = \lambda + \rho$ if and only if p divides the integer $\langle \lambda + \rho, \alpha \rangle$. On the other hand, $p > h$ implies $\langle \lambda + \rho, \alpha \rangle < p^2$ by our above remarks, so no higher power of p could divide $\langle \lambda + \rho, \alpha \rangle$. Similarly,

[9] Indeed, $p \neq 2$ will do for A_1, and for all other types $p \neq 2, 3$ is adequate: cf., J. E. Humphreys, "Algebraic groups and modular Lie algebras," *Amer. Math. Soc. Mem.* **71** (1967), Lemma 3.2.

no $\langle \rho, \alpha \rangle$ is divisible by p; so we conclude from Weyl's formula that p-dim V_λ is as stated.

COROLLARY 6.2. *Let $p > h$. Then $\lambda \sim \mu$ in Λ implies p-dim $V_\lambda = p$-dim V_μ.*

Proof. The number of reflections fixing $\lambda + \rho$ in Λ is evidently the same as the number fixing $\mu + \rho$ $(=(\lambda + \rho)^\sigma$ for some $\sigma \in W)$, so the corollary follows from Proposition 6.1.

THEOREM 6.3. *Let $p > h$. If $\lambda \in \Lambda$, then p-dim $V_\lambda \leqslant p$-dim M_λ.*

Proof. It is customary to partially order Λ_0 by the relation: $\lambda \prec \mu$ iff $\lambda - \mu = \Sigma c_i \alpha_i$, where the c_i are all nonnegative *integers*. We enlarge this relation by requiring only that c_i be nonnegative rational numbers, thereby allowing more pairs of weights to be compared. Because of the assumption $p > h$, all composition factors of $\bar{V}_\lambda$ have highest weights which are linked (Propositions 1.1 and 1.2, Theorem 4.1), and except for the highest weight λ of the top composition factor M_λ, all such weights are dominant in Λ_0, but lower than λ in the (usual) partial ordering. But such a weight might fail to be in Λ (see example below)! Nonetheless, we proceed to prove the theorem by using induction on the (enlarged) partial order and taking as our starting point the obvious fact that for $\lambda = 0$, $\bar{V}_0 = M_0$ satisfies Theorem 6.3. It must be noted here that every dominant weight is a nonnegative rational combination of the simple roots (consult the lists in [2], for example). We also use this fact as follows. Suppose a dominant weight μ *not* in Λ occurs as highest weight of a composition factor of $\bar{V}_\lambda$. Using the notation of Section 5, $\mu = \mu_0 + p\mu_1 + p^2\mu_2 + \cdots$. But all the μ_i are dominant, so we see that $\mu - \mu_0$ is a nonnegative rational combination of the simple roots, i.e., $\mu_0 \prec \mu$. We showed in Section 5 that M_μ, as $\mathfrak{g}$ module, is just a direct sum of copies of the $\mathfrak{g}$-module M_{μ_0}, so any power of p dividing the dimension of the latter surely divides the dimension of the former. But our induction hypothesis tells us that p-dim $V_{\mu_0} \leqslant p$-dim M_{μ_0}. If, on the other hand, μ is already in Λ, we get a similar statement by direct appeal to the induction hypothesis. Now, in either case, the weight μ_0 or μ is linked to λ, so Corollary 6.2 implies that p-dim $V_\lambda = p$-dim V_{μ_0} (or p-dim V_μ). Combining these arguments, we conclude that each composition factor of $\bar{V}_\lambda$ below the top one has dimension divisible by at least the power of p dividing dim V_λ. Evidently this forces the same to be true for M_λ. Q.E.D.

Consider again the definition of "defect" of a block B, $p > h$. Among all weights $\lambda \in \Lambda$ belonging to the block B, choose one for which p-dim V_λ is as small as possible, and let λ be minimal in our partial order relative to this property. Then an examination of the preceding proof shows at once that

p-dim $V_\lambda = p$-dim M_λ for this choice of λ. Accordingly, we could have defined defect more intrinsically by looking just at the dimensions of the M_λ. (This is similar to the situation for modular group algebras [7, 86.5].)

EXAMPLE. Take the root system G_2, with $p = 11$. If α_1 is the short simple root, set $\lambda = 7\lambda_1 + 10\lambda_2$. Then the dominant weight $\mu = 15\lambda_1 + 2\lambda_2$ occurs in V_λ, since $\lambda - \mu = 8(\alpha_1 + \alpha_2)$ and the length of the corresponding weight string is $\langle \lambda, \alpha_1 + \alpha_2 \rangle + 1 = 38$. If σ is reflection relative to $\alpha_1 + \alpha_2$, the condition $(\mu + \rho)^\sigma = \lambda + \rho \pmod{11}$ is satisfied. This makes μ a possible candidate for highest weight of a G-composition factor of $\bar{V}_\lambda$ (Theorem 5.1), even though $\mu \notin \Lambda$.[10]

7. CONCLUDING REMARKS AND EXAMPLES

(1) Whenever its conclusion is valid, Theorem 4.1 strengthens considerably the criterion developed by Curtis for the equality dim V_λ = dim M_λ.[11] Namely, $\bar{V}_\lambda = M_\lambda$ whenever no dominant weight $\mu \neq \lambda$ in V_λ satisfies a congruence $\lambda + \rho = (\mu + \rho)^\sigma \pmod{p}$ in Λ_0, hence whenever no corresponding congruence holds between the lengths of $\lambda + \rho$ and $\mu + \rho$ (suitably normalized). Recently, W. J. Wong[12] has devised a necessary and sufficient condition for the equality dim V_λ = dim M_λ, based on divisibility by p of a certain discriminant. However, this condition can be quite laborious to check.

(2) It might be interesting to define "vertex" and "source" of an arbitrary indecomposable $\mathscr{U}$ module, by analogy with the case of modular group algebras [7, Section 65]. In order to do this, however, one needs to understand better the structure of *induced* modules for $\mathscr{U}$.

(3) In order to decide how far our theorems go in case p is not bigger than the Coxeter number, it is important to look at low ranks for small primes. Take type A_1, $p = 2$. Here there are only two linkage classes; the one corresponding to the Steinberg module yields an entire block (as always), so the remaining class is relegated to a second block. So all the results of Sections 3–6 carry over to this case. The two-dimensional (Steinberg) module is just the usual representation, and it gets repeated twice in $\mathscr{U}$. The trivial module occurs twice in Z_0 and four times in its PIM, which only occurs once in $\mathscr{U}$.

[10] Remark: Here $p = 11$ is greater than the Coxeter number $h = 6$.

[11] See [5, Theorem 1]. This criterion is also deducible under less stringent restrictions on p from [13, Corollary 4.8].

[12] W. J. WONG, "Representations of Chevalley groups in characteristic p," Univ. of Notre Dame preprint.

Next consider the case of A_2, $p = 2$. Here there are two linkage classes; as in the preceding example, this forces existence of two blocks, which is enough to make Sections 3–5 go through. The four irreducible modules in characteristic 0 whose highest weights are restricted all remain irreducible mod 2.[13] Besides the trivial module, we have two three-dimensional modules (the usual representation and its dual) and the eight-dimensional Steinberg module (adjoint representation).

The case of A_2, $p = 3$, is more complicated. There are four linkage classes, which we group together in Table I, abbreviating $r\lambda_1 + s\lambda_2$ by (r, s).

TABLE I

Weight λ	dim V_λ
(0, 0)	1
(1, 1)	8
(1, 0)	3
(0, 2)	6
(2, 1)	15
(0, 1)	3
(2, 0)	6
(1, 2)	15
(2, 2)	27

All modules except the adjoint representation module $\mathfrak{g}$ (highest weight (1,1)) apparently have the same dimension as in characteristic 0, thus pinning down all $d_{\lambda\lambda}$ for the last three linkage classes. There are, in any case, exactly four blocks (making the results of Sections 3–5 valid here): The center of $\mathfrak{g}$ provides us with an "extra" invariant of degree 1, which along with the usual Casimir element of degree 2 generates the semisimple part of $\mathscr{C}$.

(4) By way of illustrating Sections 3–6, we list below some data for A_2 when $p = 5$, a case which is covered by our theorems. The computation of the matrix D (Theorem 4.5) is already a bit tricky in this simple case, and no algorithm suggests itself in general. Linkage classes are grouped together in Table II. Weyl's formula yields dim V_λ, while Braden's work [3] yields dim M_λ. Theorems 2.2 and 4.1 (with Proposition 1.5) and some easy diophantine equations determine the $d_{\lambda\lambda}$.

(5) It would be very desirable to find a proof for Theorem 3.1 not requiring any special condition on p. It would also be interesting to devise an algorithm

[13] Use, for example, the fact that a module all of whose weights are W conjugate must remain irreducible mod p for all p [1, 5.12].

TABLE II

Weight λ	dim V_λ	dim M_λ	$d_{\lambda\lambda}$
(0, 0)	1	1	2
(2, 0)	6	6	2
(0, 2)	6	6	2
(1, 3)	24	18	1
(3, 1)	24	18	1
(3, 3)	64	63	1
(1, 0)	3	3	2
(0, 1)	3	3	2
(1, 1)	8	8	2
(2, 2)	27	19	1
(2, 3)	42	39	1
(3, 2)	42	39	1
(0, 3)	10	10	2
(4, 0)	15	15	1
(3, 4)	90	90	1
(3, 0)	10	10	2
(0, 4)	15	15	1
(4, 3)	90	90	1
(1, 2)	15	15	2
(4, 1)	35	35	1
(2, 4)	60	60	1
(2, 1)	15	15	2
(1, 4)	35	35	1
(4, 2)	60	60	1
(4, 4)	125	125	1

for determining the matrix D, but at this point there seems to be no good reason to expect a workable algorithm to exist. Finally, the problem of finding a Weyl character formula in characteristic p seems to be as open as ever; does there, for example, exist any "reasonable" formula for dim M_λ ($\lambda \in \Lambda$) comparable to Weyl's formula in characteristic 0?

ACKNOWLEDGMENT

For several useful conversations I wish to thank B. Braden, N. Burgoyne, C. W. Curtis, T. A. Springer, and R. Wilson.

REFERENCES

1. A. BOREL, Properties and linear representations of Chevalley groups, *in* "Seminar on Algebraic Groups and Related Finite Groups" Lecture Notes in Mathematics No. 131, Springer-Verlag, Berlin, 1970.
2. N. BOURBAKI, "Groupes et algèbres de Lie," Chaps. IV–VI, Hermann, Paris, 1969.
3. B. BRADEN, Restricted representations of classical Lie algebras of types A_2 and B_2, *Bull. Amer. Math. Soc.* **73** (1967), 482–486.
4. B. BRADEN, Irreducible representations of Lie algebras of classical type, unpublished manuscript.
5. C. W. CURTIS, On the dimensions of the irreducible modules of Lie algebras of classical type, *Trans. Amer. Math. Soc.* **96** (1960), 135–142.
6. C. W. CURTIS, Representations of Lie algebras of classical type with application to linear groups, *J. Math. Mech.* **9** (1960), 307–326.
7. C. W. CURTIS AND I. REINER, Representation theory of finite groups and associative algebras, *in* "Pure and Applied Mathematics," Vol. XI, Interscience, New York, 1962.
8. J. E. HUMPHREYS, Modular representations of classical Lie algebras, *Bull. Amer. Math. Soc.* **76** (1970), 878–882.
9. M. NAGATA, Invariants of a group in an affine ring, *J. Math. (Kyoto)* **3** (1964), 369–377.
10. R. D. POLLACK, Restricted Lie algebras of bounded type, *Bull. Amer. Math. Soc.* **74** (1968), 326–331.
11. J. R. SCHUE, Symmetry for the enveloping algebra of a restricted Lie algebra, *Proc. Amer. Math. Soc.* **16** (1965), 1123–1124.
12. Séminaire École Normale Supérieure 1954/55, "Sophus Lie," "Théorie des Algèbres de Lie," Secrétariat Mathématique, Paris, 1955.
13. T. A. SPRINGER, Weyl's character formula for algebraic groups, *Invent. Math.* **5** (1968), 85–105.
14. R. STEINBERG, Representations of algebraic groups, *Nagoya Math. J.* **22** (1963), 33–56.
15. R. STEINBERG, "Lectures on Chevalley Groups" (mimeograph), Yale Univ., New Haven, Conn., 1968.
16. D. N. VERMA, "Structure of Certain Induced Representations of Complex Semisimple Lie Algebras," Dissertation, Yale University, New Haven, Conn., 1966.
17. D. N. VERMA, Structure of certain induced representations of complex semisimple Lie algebras, *Bull. Amer. Math. Soc.* **74** (1968), 160–166.